

⑤ 7243 5-8-01

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-96252

(43) 公開日 平成11年(1999) 4月 9日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 19/00		G 0 6 F 15/30	L
15/00	3 3 0	15/00	3 3 0 F
17/60		15/21	3 1 0 Z
G 0 6 T 7/00			3 4 0 B
		15/30	C
審査請求 未請求 請求項の数 1 O L (全 8 頁) 最終頁に続く			

(21) 出願番号 特願平9-251645

(22) 出願日 平成9年(1997) 9月17日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(71) 出願人 000153524

株式会社日立情報ネットワーク

東京都品川区南大井六丁目26番 3 号

(72) 発明者 吉岡 義高

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報システム事業部内

(72) 発明者 三輪 幸生

東京都千代田区大手町二丁目 6 番 2 号 株

式会社日立情報ネットワーク内

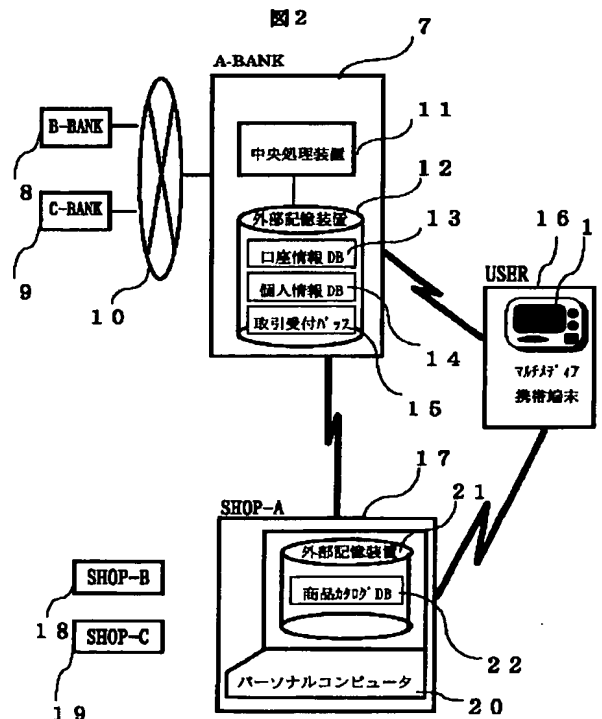
(74) 代理人 弁理士 小川 勝男

(54) 【発明の名称】 マルチメディア携帯端末を用いた電子マネー取引方式

(57) 【要約】 (修正有)

【課題】 マルチメディア携帯端末という利用する場所を特定しない装置を用い、網膜パターンと指紋という各個人独特かつ変造不可能な情報の組み合わせによって本人認証を行い、その認証をパスした利用者のみが商取引を行うことができる。

【解決手段】 利用者はマルチメディア携帯端末1から商店17にアクセスし商取引を行ない、両者は自分の口座番号を相手にはわからないように暗号化し取引結果に付加して取引相手に送信し、それぞれが相手から送信された情報に自分の暗号キーを付加して銀行7に転送する。銀行は両者が送信してきた情報をそれぞれの取引相手が添付してきた暗号キーを用いて取引結果を解読し、利用者が送信してきた取引の購入金額と商店が送信してきた販売金額が一致していることを確認し、一致している場合のみ口座振替を行う。



【特許請求の範囲】

【請求項 1】利用者はマルチメディア携帯端末より、商店のパーソナルコンピュータにアクセスし、自分の口座残高の範囲内で取引を行うシステムにおいて、前記携帯端末を用い網膜パターンと指紋を採取し、それをあらかじめ銀行に登録してある個人情報と比較して本人認証を行ない、問題無ければ自分の口座残高情報を得た前記携帯端末を利用し、希望する商品選択後、商店に暗号化した自分の口座番号を送信し、商店はそれに自分の暗号キーを付加して銀行に送信し、また商店は利用者に暗号化した自分の口座番号を送信し、利用者はそれに自分の暗号キーを付加して銀行に送信し、銀行では、それぞれの暗号キーによって口座番号の解読をし、銀行では商店から送信してきた販売金額と利用者から送信してきた購入金額が一致したときのみ口座振替を行ない決済することを特徴とする電子マネー取引方式。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、利用する場所を特定しない使い勝手の良さと高いセキュリティが必要な電子マネー取引。

【0002】

【従来の技術】例えば、従来の電子マネー取引方式としては、特開平 3 - 9 2 9 6 6 号公報に記載されるように、銀行の特定の装置より IC カードのような媒体に残高情報を書き込み、利用者は商店等に出向き前記媒体を用いて取引を行う。商店側は、商店内の集計ファイルに記憶され、その取引結果を銀行に送信し、銀行は該当口座どうしの振替によって決済を行う方式、または取引相手の氏名や口座番号など個人情報を指定することで銀行内で口座振替を行う方式などが挙げられる。

【0003】

【発明が解決しようとする課題】前記のような方式においては、利用者が商店に出向くかもしくは取引を行う場所が特定されてしまう、商店から銀行に集計ファイルを送信するといった現金としての致命的な欠陥であるリアルタイム取引ができない、IC カード等の物理的な機構のみに依存しているために複製される可能性がでく、商店が銀行に対し利用者の購入した金額より高い金額を請求したり、第 3 者によって情報が書き換えられたりされていない保証の無いまま口座振替が行われてしまう、本来の現金での商取引の概念と違って取引相手の個人情報に相手に対し公開されないと商取引が行えないなどといった欠点がある。

【0004】そこで本発明の目的は、ユーザの使い勝手の良さと安心して利用できる高いセキュリティをもった電子マネー取引方式を提供することである。

【0005】

【課題を解決するための手段】本題において開示される発明のうち、代表的なものの概要を簡単に説明すれば下

記のとおりである。

【0006】すなわち、本発明の電子マネー取引方式は、マルチメディア携帯端末という利用する場所を特定しない装置を用い、網膜パターンと指紋という各個人独特かつ変造不可能な情報の組み合わせによって本人認証を行い、その認証をパスした利用者のみが商取引を行うことができる。その商取引においても、利用者は前記携帯端末から商店にアクセスし商取引を行ない、両者は自分の口座番号を相手にはわからないように暗号化し取引結果に付加して取引相手に送信し、それぞれが相手から送信された情報に自分の暗号キーを付加して銀行に転送する。銀行は両者が送信してきた情報をそれぞれの取引相手が添付してきた暗号キーを用いて取引結果を解読し、利用者が送信してきた取引の購入金額と商店が送信してきた販売金額が一致していることを確認し、一致している場合のみ口座振替を行う。

【0007】

【発明の実施の形態】以下、本発明による電子マネー取引方式の一実施例を図面を用いて詳細に説明する。

【0008】図 1 は本発明の電子マネー取引方式に用いるマルチメディア携帯端末の外観概略図、図 2 は本実施例である電子マネー取引システムの概略構成図、図 3 は本実施例における銀行内の中央処理装置と接続された外部記憶装置にある口座情報データベースの内容を示す説明図、図 4 は本実施例における前記外部記憶装置にある個人情報データベースの内容を示す説明図、図 5 は本実施例における前記外部記憶装置にある売買取引照合用作業領域の内容を示す説明図、図 6 は本実施例における商店内のパーソナルコンピュータに接続された外部記憶装置にある商品カタログデータベースの内容を示す説明図、図 7 は本実施例における本人認証によって銀行と端末間で残高確認動作を示すフローチャート図、図 8 は本実施例の電子マネー取引システムでの電子マネー取引方式を示すフローチャート図である。

【0009】まず、図 2 により本実施例の電子マネー取引システムの構成を説明する。

【0010】本実施例の電子マネー取引に用いるマルチメディア携帯端末 1 は、タッチパネル入力機能付きディスプレイ 2、CCD カメラ 3、マイク 4、スキャナ 5、スピーカ 6 を備えた装置で、銀行や商店などに無線通信によってアクセスする機能を有する。無線通信を行う際、利用者は自分の電話番号を暗号化して送信し、送信相手に自分の電話番号を知られることなく返信させることができる機能も有している。

【0011】A - BANK 7 の中央処理装置 11 に接続された外部記憶装置 12 は、外部からアクセスされることは絶対になく、書き込みや読み出しは接続された中央処理装置からのみである。前記外部記憶装置には、A - BANK の預金者の口座番号データ 24、氏名データ 25、残高データ 26 の情報を持った口座情報データベ

ス13、A-BANK預金者の詳細な個人情報を持った個人情報データベース14、商取引が行われた際、SHOP-A17が送信してきた販売データ39とUSER16が送信してきた購入データ43の照合を行いUSERの口座番号47とSHOP-Aの口座番号を算出する取引受付バッファ15領域を格納している。

【0012】SHOP-A17のパーソナルコンピュータ20は、マルチメディア携帯端末1の利用者が無線通信を行う際、自分の電話番号を暗号化して送信し、送信相手に自分の電話番号を知られることなく返信させることができる機能に対応しているため、端末への返信時に相手の電話番号を意識する必要はない。

【0013】また、同パーソナルコンピュータに接続されている外部記憶装置21には、その店が扱っている商品のカタログデータベース22が格納されている。

【0014】A-BANKは、金融機関ネットワーク10に接続されており、ネットワークに同様に接続されたB-BANK8やC-BANK9といった他の金融機関ともデータのやり取りを行うことができる。

【0015】SHOP-Aと同様のシステムが、SHOP-B18やSHOP-C19のように複数の商店に存在する。

【0016】次に、本実施例の作用について、電子マネー取引システムの動作フローを図8により説明する。

【0017】始めに、ステップ801で、USERは携帯端末より商品購入指示をだす。

【0018】次に携帯端末利用者がUSER本人に間違いがないか以下の手順で本人認証を行う。

【0019】ステップ702において、マルチメディア携帯端末のCCDカメラ3で網膜パターンを採取し、それと同時にスキヤナ5で指紋の採取も行う。

【0020】ステップ703において、ステップ702で採取したUSERの網膜パターンと指紋を、A-BANKに対してUSERとA-BANKで独自に定められたアルゴリズムで暗号化して送信する。

【0021】ステップ704では、ステップ703で受信した網膜パターンと指紋のデータと、予め口座開設時に登録された個人情報データベース内のUSER網膜パターンデータ35とUSER指紋データ36を、ステップ705で照合して本人認証を行う。

【0022】もし、本人認証にパスすれば、ステップ706でA-BANKは、USERに対して口座情報データベース内のUSER残高情報31を前記のアルゴリズムによって暗号化しUSERに返信する。

【0023】また、本人認証で異常が発見された場合は、ステップ708においてBANK-AはUSERに対し、本人認証が失敗したことを伝え、エラーを表示して終了する。

【0024】本人認証が正常にパスされれば、USERの残高情報を表示する。その際、本取引はリアルタイム

処理のため2重取引は考えられないが、念のため前回に行った商取引の決済が完了するまで待ってから残高情報を返信しない仕様とする。

【0025】そして、ステップ804においてUSERはSHOP-Aに無線通信によってアクセスしSHOP-Aの商品カタログデータベース22より選択し、その際に、ステップ805においてUSERは自分の購入した商品の購入金額を携帯端末に記憶し、SHOP-Aに対しては自分の口座番号に乱数を使ったユニークなUSER暗号キー45を加算して送信する。

【0026】SHOP-Aは、ステップ807において自分の販売した商品の販売金額を携帯端末に記憶し、ステップ808においてパーソナルコンピュータ20の前記の相手の電話番号がわからなくても返信できる機能を用い、USERに対して自分の口座番号に乱数を使ったユニークなSHOP-A暗号キー41を加算して返信する。

【0027】次に、USERはステップ809において、ステップ808にて送信されてきた取引の購入金額、SHOP-Aの暗号化された口座番号とステップ806にて生成したUSER暗号キーを添付してBANK-Aに送信する。

【0028】また、SHOP-Aは、ステップ810において、ステップ806にて送信されてきた取引の販売金額、SHOP-Aの暗号化された口座番号とステップ808にて生成したSHOP-A暗号キーを添付してBANK-Aに送信する。

【0029】BANK-Aでは、ステップ811において、USERが送信してきた購入金額とSHOP-Aが送信してきた販売金額を比較し、もし一致しなければステップ814において、BANK-AからUSERとSHOP-Aに対し口座振替え情報に異常があることを連絡し、商取引が無効である事を知らせる。

【0030】また、ステップ811において、USERが送信してきた購入金額とSHOP-Aが送信してきた販売金額を比較し、一致すればステップ812において、BANK-Aは、暗号化されたSHOP-Aの口座番号44（SHOP-Aの口座番号+SHOP-A暗号キー）を商品販売データ39のSHOP-A暗号キー41を用いて解読し、SHOP-A口座番号48に格納する。

【0031】さらに、ステップ812において、BANK-Aは、暗号化されたUSERの口座番号39（USERの口座番号+USER暗号キー）を利用者購入データ43のUSER暗号キー45を用いて解読し、USER口座番号47に格納する。

【0032】両者の口座番号を上記によって算出した後、取引金額（=販売金額=購入金額）をSHOP-Aの口座からUSERの口座へ振替え、口座情報データベース内のUSER残高31とSHOP-Aの残高32を

10

20

30

40

50

書き換える。

【0033】その後、ステップ813においてBANK-Aから、USERとSHOP-Aに対し処理が正常終了したこと送信し電子マネー取引を完了する。

【0034】以上、1取引の時について説明したが、同時に複数の取引が発生した場合は、銀行は取引ナンバーにより管理する。

【0035】

【発明の効果】以上説明したように本発明のうち代表的なものによって得られる効果を説明すれば、下記のとおりである。

【0036】(1). マルチメディア携帯端末を用いることで電子マネー取引を行う場所を特定することなく、網膜パターンと指紋という各個人独特かつ変造不可能な情報の組み合わせによって本人認証を行うことで、ユーザの使い勝手の良さと、他者に悪用されることのないセキュリティの高いシステムが提供できる。

【0037】(2). 氏名や口座番号を取引相手に公開しないといった現金本来の商取引と同様の概念でマネー取引が実現できる。通常、氏名や口座番号のみでは、銀行口座を操作することはできないが、取引を行った利用者の氏名や口座番号など個人情報を使って犯罪が行われたり、商店が利用者の個人情報を得ることでユーザは希望もしないダイレクトメールの対象にされることを防止するといったプライバシーの保護・個人情報の不正使用の防止ができるシステムが提供できる。

【0038】(3). 銀行の口座振替えにあたって、商店や利用者の取引データの故意の書き換えや、データ化けといった偶然のデータの変更がチェックでき、間違った口座振替え処理が行われない。

【図面の簡単な説明】

【図1】本発明の電子マネー取引方式に用いる マルチメディア携帯端末の外観概略図である。

【図2】本発明の電子マネー取引方式の一実施例である電子マネー取引システムの概略構成図である。

【図3】本実施例において、銀行内の中央処理装置と接続された外部記憶装置にある口座情報データベースの内容を示す説明図である。

【図4】本実施例において、銀行内の中央処理装置と接続された外部記憶装置にある個人情報データベースの内容を示す説明図である。

【図5】本実施例において、銀行内の中央処理装置と接続された外部記憶装置にある売買取引照合作業領域の内容を示す説明図である。

【図6】本実施例において、商店内のパーソナルコンピュータの外部記憶装置にある商品カタログデータベースの内容を示す説明図である。

【図7】本実施例において、本人認証によって銀行と端末間で残高確認動作を示すフローチャート図である。

【図8】本実施例の電子マネー取引システムにおい

て、電子マネー取引引き方式を示すフローチャート図である。

【符号の説明】

- | | |
|----|-----------------------------|
| 1 | マルチメディア携帯端末 |
| 2 | タッチパネル入力機能付きディスプレイ |
| 3 | CCDカメラ |
| 4 | マイク |
| 5 | スキャナ |
| 6 | スピーカ |
| 10 | 7 銀行（説明用 A-BANK） |
| | 8 銀行（説明用 B-BANK） |
| | 9 銀行（説明用 C-BANK） |
| | 10 金融機関ネットワーク |
| | 11 中央処理装置 |
| | 12 外部記憶装置（パーソナルコンピュータ |
| | 13 口座情報データベース |
| | 14 個人情報データベース |
| | 15 取引受付バッファ |
| | 16 マルチメディア携帯端末ユーザ（説明用 本取引 |
| 20 | システム利用者） |
| | 17 商店（SHOP-A） |
| | 18 商店（SHOP-B） |
| | 19 商店（SHOP-C） |
| | 20 パーソナルコンピュータ |
| | 21 外部記憶装置（パーソナルコンピュータ接続） |
| | 22 商品カタログデータベース |
| | 24 口座情報データベース内 口座番号データ |
| | 25 口座情報データベース内 氏名データ |
| | 26 口座情報データベース内 残高データ |
| 30 | 27 USER（説明用 本取引システム利用者）口座番号 |
| | 28 SHOP-A（説明用 商店）口座番号 |
| | 29 USER（説明用 本取引システム利用者）氏名 |
| | 30 SHOP-A（説明用 商店）氏名〔商店名〕 |
| | 31 USER（説明用 本取引システム利用者）口座残高 |
| | 32 SHOP-A（説明用 商店）口座残高 |
| | 33 個人情報データベース内 口座番号データ |
| | 34 個人情報データベース内 氏名データ |
| | 35 個人情報データベース内 網膜パターンデータ |
| | 36 個人情報データベース内 指紋データ |
| 40 | 37 個人情報データベース内 住所データ |
| | 38 個人情報データベース内 TELデータ |
| | 39 取引受付バッファ内 商品販売データ領域 |
| | 40 取引受付バッファ内 暗号化利用者データ領域 |
| | 41 取引受付バッファ内 商店暗号キーデータ領域 |
| | 42 取引受付バッファ内 商品販売金額データ領域 |
| | 43 取引受付バッファ内 利用者購入データ領域 |
| 50 | 44 取引受付バッファ内 暗号化商店データ領域 |

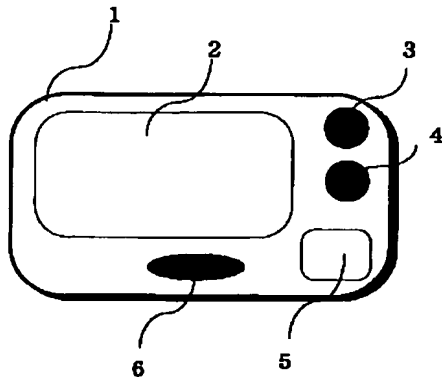
- 4 5 取引受付バッファ内 利用者暗号キーデータ 領域
- 4 6 取引受付バッファ内 利用者購入金額データ 領域
- 4 7 取引受付バッファ内 利用者口座番号算出結果記憶領域
- 4 8 取引受付バッファ内 商店口座番号算出結果 *

* 記憶領域

- 4 9 商品カタログデータベース内 商品-大分類
- 5 0 商品カタログデータベース内 商品-小分類
- 5 1 商品カタログデータベース内 商品-商品番号
- 5 2 商品カタログデータベース内 商品-商品名
- 5 3 商品カタログデータベース内 商品-単価
- 5 4 商品カタログデータベース内 商品-PR情報

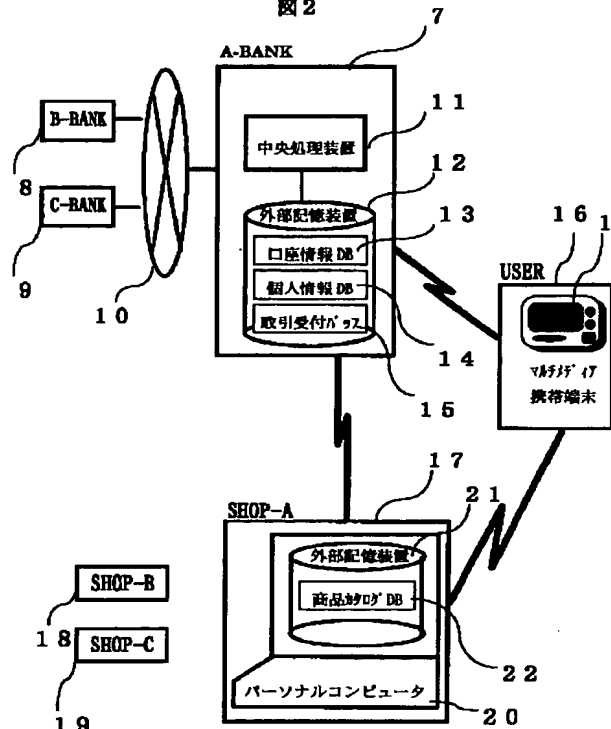
【図 1】

図 1



【図 2】

図 2



【図 3】

図 3

口座番号	氏名	残高
USER 口座番号	USER NAME	USER 残高
...
SHOP-A 口座番号	SHOP-A	SHOP-A 残高
...

【図 4】

図 4

口座番号	: USER 口座番号
氏名	: USER NAME
網膜パターン	: USER 網膜パターンデータ
指紋	: USER 指紋データ
住所	: USER 住所データ
TEL	: USER TELデータ

【図 5】

図 5

1 5

3 9

4 0

4 1

4 2

商品 販売データ

USER口座番号 + USER 暗号

SHOP 暗号キー

販売金額

4 3

4 4

4 5

4 6

利用者 購入データ

SHOP口座番号 + SHOP 暗号

USER 暗号キー

購入金額

4 7

4 8

USER 口座番号

SHOP 口座番号

【図 6】

図 6

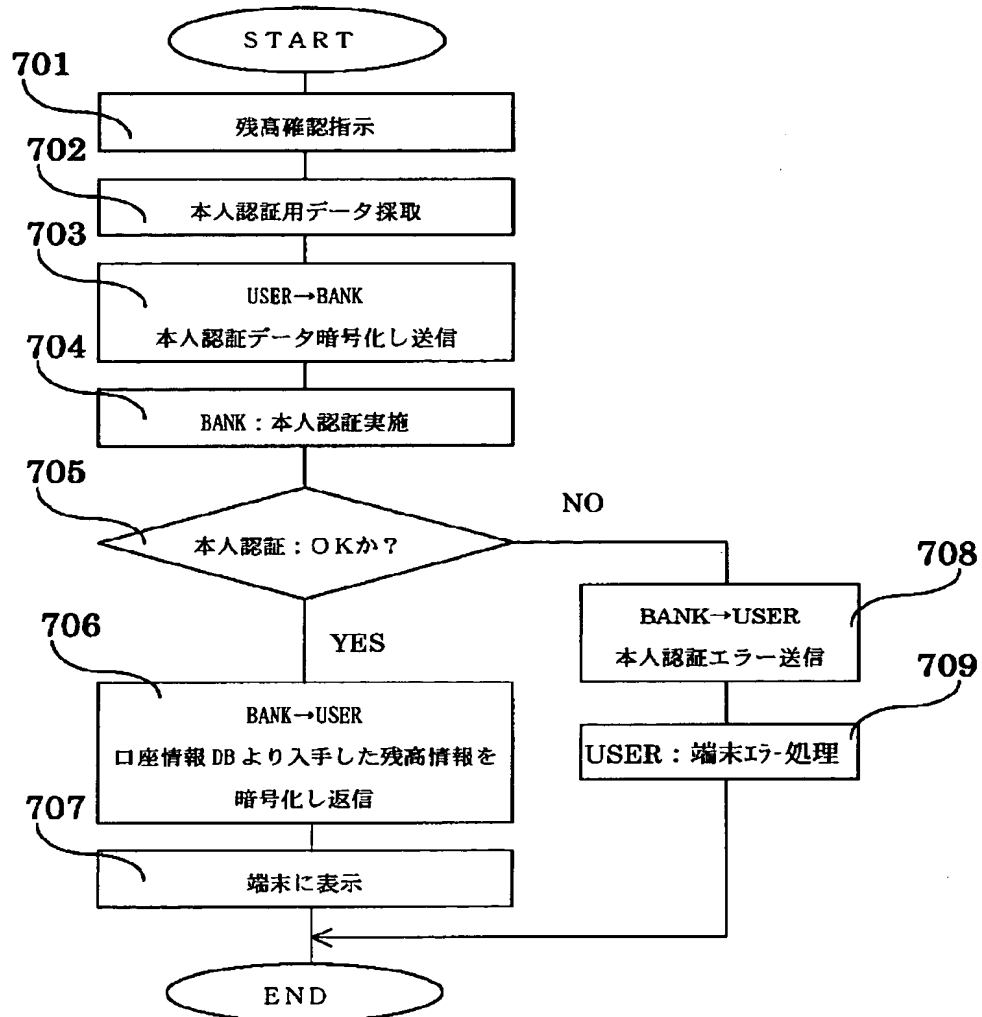
2 2

4 9 5 0 5 1 5 2 5 3 5 4

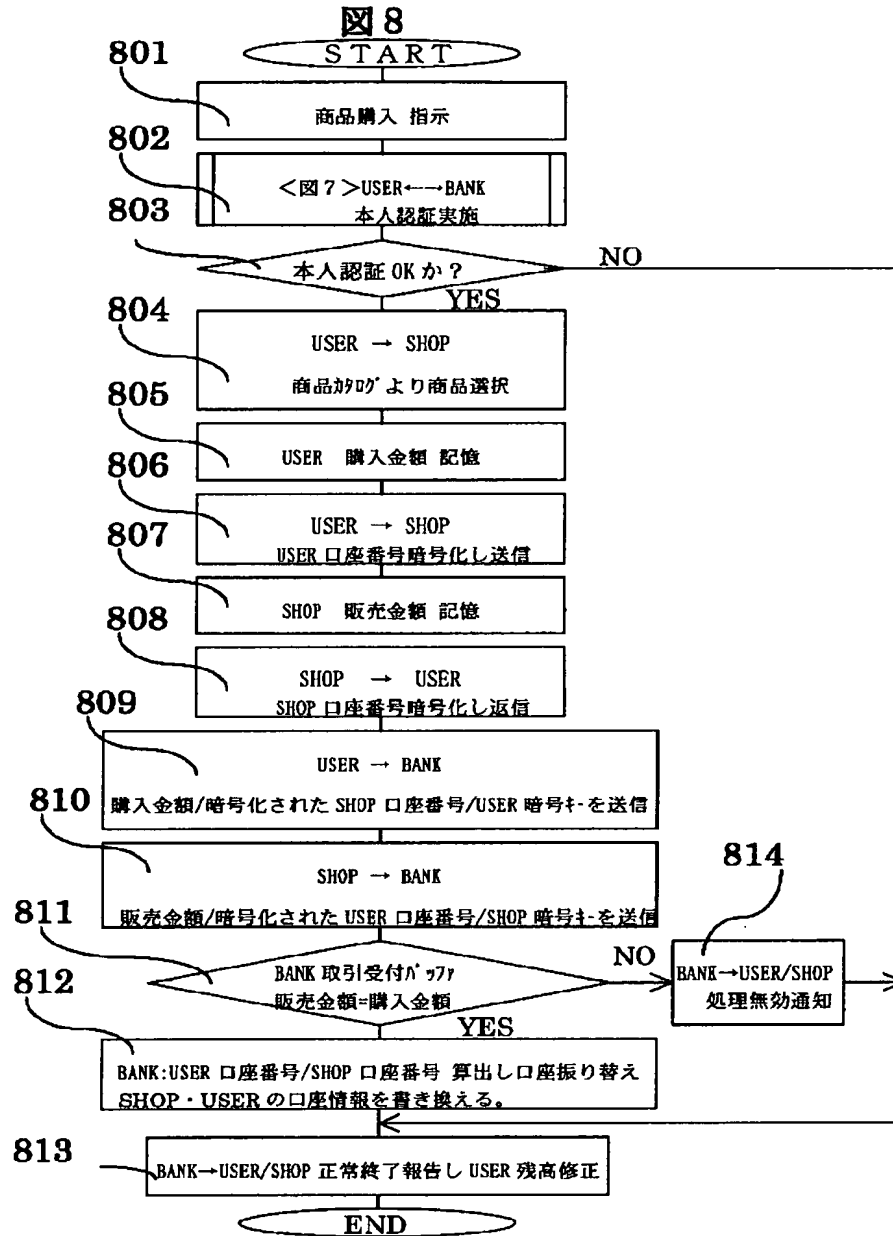
大分類	小分類	商品番号	商品名	単価	PR
:	:	:	:	:	:
:	:	:	:	:	:
:	:	:	:	:	:
:	:	:	:	:	:

【図 7】

図 7



【図 8】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

F I

G 0 6 F 15/30

3 4 0

15/62

4 6 0



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11096252 A**(43) Date of publication of application: **09.04.99**

(51) Int. Cl.

G06F 19/00**G06F 15/00****G06F 17/60****G06T 7/00**(21) Application number: **09251645**(22) Date of filing: **17.09.97**(71) Applicant: **HITACHI LTD HITACHI
INFORMATION NETWORK LTD**(72) Inventor: **YOSHIOKA YOSHITAKA
MIWA YUKIO****(54) ELECTRONIC MONEY TRANSACTION SYSTEM
USING MULTIMEDIA PORTABLE TERMINAL**

(57) Abstract:

PROBLEM TO BE SOLVED: To enable only user who passes personal authentication to perform business trade by performing the personal authentication by using a device whose place of use is not restricted like a multimedia portable terminal and by combination of information which is unique to an individual and impossible to be forged like a retina pattern and a fingerprint.

SOLUTION: The business trade is performed by making access from the multimedia portable terminal 1 to a store 17 by a user, their own bank account numbers are ciphered so as not to be known to the opposite party, added to a trade result, transmitted to the opposite party of the trade by both of the user and the store, own ciphered keys each is added to the information transmitted from the opposite party and the information is transmitted to a bank 7 by each of the user and the store. The trading result of the information transmitted from both of the user and the store are deciphered by using a ciphering key attached by each party of the trade, coincidence of a purchasing amount of the trade transmitted by the user with a sale amount transmitted by the store is confirmed and the amount is transferred from the bank account only when the amounts coincide with each other by the bank.

COPYRIGHT: (C)1999,JPO

